Massachusetts State Police

Office of the Attorney General
One Ashburton Place, Room 1910
Boston, MA 02108

To:	Lieutenant Stephen Matthews, Commanding, A.G.O.
From:	Trooper David W. Crouse #0839 A.G.O.
Subject:	Interview at CCBN with Buckley, Jason and Gendreau, Michael
Case Number:	02-034-2399-0087

1. On Thursday, April 4, 2003 this officer along with Lt Dermot Quinn went to CCBN located at 343 Congress St, Boston, Ma. While at CCBN these officers had the opportunity to speak with Buckley, Jason and via telephone conference Gendreau, Michael. Also present was Nassar, Nicandra, Corporate Counsel for CCBN. Buckley and Gendreau are employed by CCBN and are responsible for the computer network at CCBN.
2. The nature of this meeting was to gain information into allegation from Shareholder. Com that someone at CCBN had accessed Shareholder.Com's management webpage. Buckley explained how the network is currently configured and that over the past year they have changed the system. We explained that we had obtained several different IP addresses assigned to CCBN in the Shareholder.Com logs. Furthermore we felt that one computer committed the access. By looking at the Shareholder.Com logs and speaking with Keith Barrett of Shareholder.Com it was discovered that the webserver at Shareholder.Com sends a cookie to a computer the first time it visits. The webserver creates a unique number for each cookie it gives out. Then each time that computer returns, the webserver checks to see if that computer has been there

before. If it has, the webserver logs that session under the old cookie id number. The fact that there is a unique cookie given to each web browser draws the conclusion that the connection is from one computer. Barrett searched his logs for the occurrence of this particular cookie, which had come in from a CCBN IP address and then provided this officer with this information. These log excerpts contain IP Addresses for CCNB and AOL proxy servers.

3. Several scenarios were hashed out of how the connection could come from both CCBN and AOL IP addresses. One was the use of terminal server the other is that the computer has been connected to the CCBN network and also has dialed up into AOL's network.

4. CCBN allows it's employees to use a service called "terminal server" Terminal services allows the employee to dial into a computer at the office and do things on the systems as if they were actually in the building. If the employee were to go out to the internet the IP address that would be captured would be that of CCBN not the IP address of the dialup into the company. The possibility of an employee using terminal server to gain access from outside of CCBN then go to Shareholder.com was ruled out. The Shareholder.com webpage passes a cookie to the browser of the computer that is viewing the webpage. When using terminal server the actual connection is made by the computer acting as the server (the computer located at CCBN) and the client computer is seeing a virtual copy of the webpage. Hence, the cookie would be left on the "server". In this case, the logs show that the computer connecting to Shareholder.com is the same cookie/browser/computer.

5. Due to the fact that the connection has been made by a CCBN and an AOL IP addressees using the same cookie it is reasonable to assume that the computer is a laptop. For a CCBN employee to connect to AOL via a dial-up connection at the office they would have to use a dedicated line and those are reserved for fax machines. CCBN's Quality and Assurance division has an AOL account, this account is typically used from the office using the AOL client and connects via LAN not dial-up. (After the interview, this officer conducted a test connecting to AOL via LAN and the IP address that would be captured was not the AOL IP.)

6. Having looked at these two scenarios it is concluded that the connections were most likely made by a laptop that has the AOL client installed. It is not reasonable to think that someone brings a desktop to and from the office. Buckley estimates that there are approximately 150 laptops in use at CCBN.

7. The IP addresses collected by Shareholder.Com were varied within CCBN class "C" IP. Buckley was unsure how this could be as their network is set up to go through a gateway that only shows one IP address to the public side of their connection to the Internet. Buckley suggested that we speak with Michael Gendreau, of the IT staff. Gendreau has been with the company for longer and has been involved in the migration of the network over the past years. Gendreau was contacted by telephone and placed on conference call.

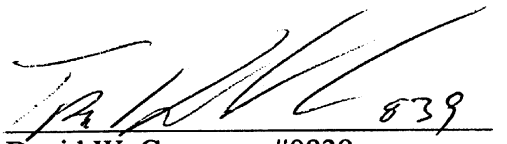
8. We explained what we were investigating and that Buckley felt that he might be able to speak better about the history of the networks configuration. Gendreau explained that for a period, about a year ago, the network had been configured differently than it is now. In the past, if a computer went to the Internet, the server assigned an IP from a block of IP addresses. The IP was randomly assigned for each session. During that session the randomly assigned IP is what would be viewed publicly on the Internet. This would explain why several IP addresses were captured by the Shareholder.Com's webserver. Gendreau stated that there was a logging feature and that it was logging during that period. However, the log was set to overwrite itself after it captured approximately 7MB of data. He stated that 7MB traditionally would be about 5-7 days of data. Furthermore, that system had been reconfigured about six months ago and the log data would have been discarded during that transition.

9. There had been several failed attempts to access the Shareholder.Com webservers. These attempts were after Shareholder.Com had hardened their security. The webserver does not capture IP addresses on failed attempts to log in. It does capture the name of the computer. Computers located in business settings traditionally have a naming convention for ease of keeping track of their inventory. Buckley explained that they use a naming convention of the users first initial and last name. Buckley printed up a list of all computers that were

connected to the network while we were there. The computers that had failed to connect were named "sales1" and "MORPEUR". It was then asked if they had/ have an employee with a similar name to M. Orpeur. Buckley, Gendreau, and Nassar indicated that they did not.

10. In conclusion, all present at the meeting concur that it appears that someone from within CCBN had accessed the Shareholder.com's secure webserver as indicated in the logs, that is most likely a laptop, and any remnants of a log that would indicate who had a specific IP on a given date and time is no longer available. The only tangible solution is that the unique cookie furnished to the suspect computer may still be on the computer.

Respectfully Submitted,



David W. Crouse #0839
Trooper, Massachusetts State Police
Office of the Attorney General